QUANTUM NETWORK PROTOCOLS

D. J. Jackson, David P. Gilliam, and J. P. Dowling
Jet Propulsion Laboratories
California Institute of Technology
4800 Oak Grove Drive
Pasadena, CA 91109

Innovative Claims for Research

The earliest quantum information processing application to be implemented will be securing fiber and free-space communications channels using qubits (defined superposition's of binary photon states) to distribute encryption keys.[1] The problem of distributing the qubits between two-nodes has essentially been solved for the Quantum Key Distribution (QKD) encryption application and current development efforts are focused on pushing key generation throughput rates to 10 Gbps. This is estimated to be about five years away. Upon realization of multi-Gigabit throughput key generation rates, QKD becomes practical for deployment onto fiber networks when combined with most encryption algorithms, and specifically with the Vernam cipher (One Time Pad). But in order to benefit from the quantum properties of photonic qubits, one must first take into account the physical, information-bearing properties of quantum particles. Unlike classical photons, all handling of the photonic qubits must be done without regeneration and without detecting the qubit state in order to prevent corruption of the qubit information.

Our objective is to examine implications of quantum properties in designing a protocol for a Quantum Internet Testbed with multiple nodes ($N > 2$) for distributing qubit particles (single polarized photons or entangled photon states) among different user nodes within a network. This will include designing a network architecture and protocol that, with the use of photonic storage buffers, allows each user node some control over the time at which it chooses to accept an input photon from the network. This effort will closely examine the implications for distributing qubits about a network and the timing control of introducing the qubits into a computational environment. It will try to come up with guidelines for how to structure a minimum datalink layer of the protocol stack for quantum computing applications. Assuming that photons are the medium used to convey qubit information, important issues that must be addressed to design a quantum compatible OSI (Open Systems Interconnection) model protocol include but are not limited to (1) Routing implications of a dis-associated (2) Physical properties controlling routing (i.e. time-to-live of qubits in network (TTLQ), short-term buffered storage of qubits, decoherence time of the qubits, non-regenerative property of qubits), (3) Scaling up from a managable number of nodes LAN, n (e.g. $2 < n \leq 20$), to N arbitrarily large, where $N = Kn >> n$ and K is the number of LANs being coupled into the network, and (4) the long term storage of qubits. The network protocols for the qubits are analogous to the first four layers of the standard OSI model. The quantum protocol will follow the TCP/IP (Transmission Control Protocol/Internet Protocol) address routing framework.

It is imperative to perform this study now because the infrastructure of the all optical networks are still being defined and are not yet fully deployed. If QKD becomes an important means of securing communications networks, then the infrastructure must be capable of disseminating and distributing qubits. These issues need to be addressed in the current research on optical networks to avoid the expense of designing them in after the fact.

Finally, we also anticipate that beyond the QKD application, a generalized quantum computer that is capable of more complex functions than key distribution will probably also use a distributed architecture. What we learn here will also lay the groundwork for qubit distribution in distributed quantum computing applications.

Background

The systems engineering decisions that led to the current digital electronic computer architecture was driven by physical electronic properties[2]. This has led to a processor that is optimized to take advantage of physical electronics and to work around the unique set of problems electronics has to offer. Specifically, electron-electron interactions limited the interconnect packing density of the computer memory until von Neumann introduced the concept of an addressable memory module. The memory, of course, serves the invaluable function of storing information until it is ready for use in computation. Also, the logic functions (AND, OR, and NOR) that form the basis of the electronic processor are based on the logic gates that are intrinsic to certain electronic devices.

It stands to reason that in evolving the architecture of a Quantum Computer, it is important to take into account the nature of physical quantum properties and the mediums used to define the qubits in order to evolve a useful architecture. To date, a variety of different media, such as atomic nuclear spins, trapped ions, cavity QED-based[3,4] gates, and photons[5,6] have been used to define the qubits to be used as quantum computing logic gates. These will eventually become the lowest level building blocks for the Quantum computing processor. . For the purposes of this investigation, we assume a distributed architecture as the baseline for the quantum computer. The quantum computing applications, which define their qubits using photons, will have the potential for easy implementation in such a distributed network. Although we do not yet know the final form that the quantum computer architecture will take, it is a reasonable assumption that the ability to control the time at which photons, distributed by the network, are introduced into any given computing engine[2] would be a critically useful function to have. The demonstration of optical storage (e.g. ultra-low loss delay loops) is thus an important next step.

The basic principles for this time-control function in the context of the Quantum Internet can be demonstrated with the Quantum Key Distribution[7] (QKD) application. QKD offers the ability to generate key sequences that can be securely distributed. This is important because the key distribution step is considered to be the weakest part of most classical encryption protocols. QKD combined with the Vernam cipher[8], offers an unconditionally secure communications protocol.

Within the last few years, QKD in fibers has been demonstrated over distances of several tens of kilometers. In particular, Townsend[9] has not only demonstrated QKD over 30 km of fiber, he has also shown that QKD works quite well when implemented in a conventional Dense Wavelength Division Multiplexed (DWDM) data transmission network. This implies that qubit distribution is currently possible in LAN, MAN, and limited WAN networks. We propose introducing QKD as the first application in our Quantum Internet Testbed, with the idea of extending the use of the testbed to demonstrate a distributed architecture for other Quantum Computing functions as they are developed and matured by other research groups.

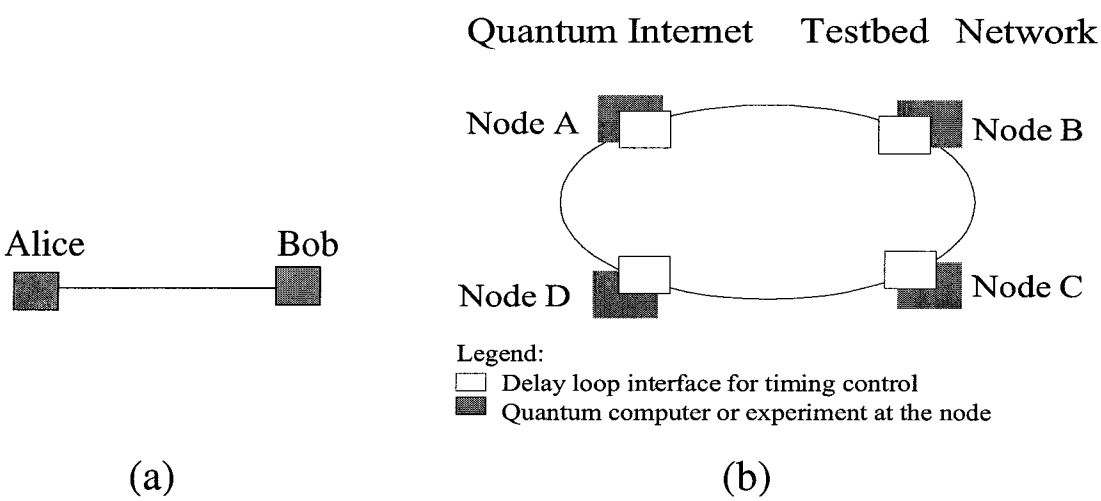

Figure 1. (a) Two-node qubit distribution channel used for Quantum Key Distribution; (b) Schematic of a Quantum Internet network illustrating the addition of photon storage delay loops that control the time at which the photons are introduced into the node.

To date, most links attempting to distribute qubits connect between two points, A and B (see Figure 1 (a)). Successful qubit delivery is accomplished in these networks with dedicated equipment through the use of timing pulses that precede the qubit and ancillary communications channels, which insure the viability of the qubit delivery. Now we would like to grow from a two node network to one containing n nodes, where $n > 2$. Ideally, such an expanded quantum distribution network will have features similar to those developed for local area networks, metropolitan area networks, and wide area networks. For example, dynamic routing capability, scalability, and a well defined time-to-live (TTL). Other features will be unique to the quantum distribution network based on the unique physical properties of the qubits. For example, it would require a header dis-associated from the information bearing qubit. Such a header would probably be part of the timing pulse and would potentially need routers capable of reduced header optical packet switching such as those being investigated at UC Santa Barbara, Princeton and MIT

Lincoln Labs.[10] Since qubits cannot be regenerated without destroying their entanglement, this network must handle all routing functions without detecting the qubit itself. Error detection does not have the same meaning when distributing qubits since the state of the qubit is probabilistic. Additionally, specialized routers capable of handling routing qubits dis-associated from the header and timing pulse need to be developed to ensure appropriate packet delivery of the qubits. Due to the time delay in reading the header information, the delivery of the qubits will have to include these and other network latency issues. Other more advanced topics include the possibility of streaming (using wavelength division multiplexing to send multiple photons in one slot) to increase the link efficiency.

Approach

Given our objective of developing a Quantum Internet Testbed with multiple nodes, N > 2, as shown in Figure 1 (b). A key feature which we would like to build into this testbed is the ability to control the time at which photons arriving from the network are actually injected into a given node for use by a Quantum processor (or by an experiment). That is devising routing protocols that provide for distribution of a qubit among a small number of nodes, n. In n = 4, this would involve distributing from node A to a selected node B, C, or D, and then some method of optically storing the photons until the selected time of injection. Our approach is to first develop a network architecture and a set of protocols that will support the accomplishment of this new time-control function. The next step is to develop a LAN breadboard. As a baseline, we will likely use a DWDM design similar to that demonstrated by Maurand and Townsend[9] where the qubits, routing packets, and timing pulses travel over the same fiber. We anticipate that there will be performance limitations due to the existing hardware, specifically with regard to the lifetime of the photon in the network. In this scenario, the maximum storage period represents the decoherence limit for photonic qubits in the network.

Scalability

Once a basic protocol is established for a LAN type network (n < 20), which is easily realizable, we will address the issues associated with scaling networks with N > 20 by coupling to multiple LAN's. For example, connecting networks as depicted in Figure 2.

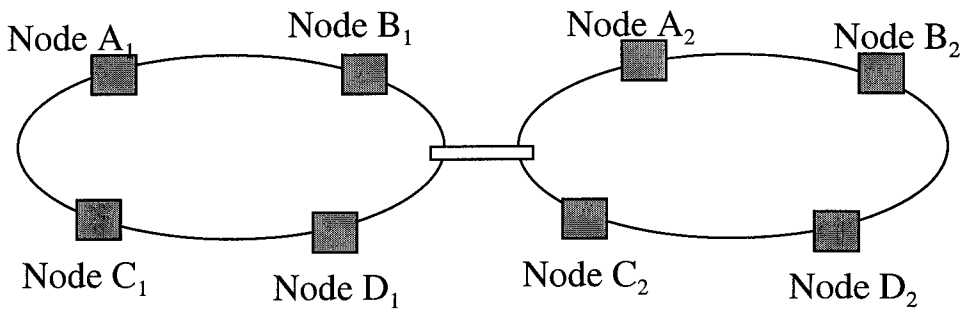

Figure 2. Schematic for scaling up in N by the multiple coupling of LAN's.

In a quantum WAN, qubits will need to be routed to their destination network without observation. We intend to examine the current research in optical technology and define a method of routing packets with dis-associated headers to multiple networks making use of the emerging technologies to provide the ability to route packets without having to examine the contents. Use of MicroElectroMechanial System (MEMS) switches and Nonlinear Optical switches as well as new small packet label optical routers as a means for providing a packet routing infrastructure will be examined.

REFERENCES

(1) G. Gilbert and M. Hamrick, "Practical Quantum Cryptography: A Comprehensive Analysis (Part One)", MITRE Technical Report (MTR 00W0000052), September 2000.
(2) D. J. Jackson, Photonic Processors: A Systems Approach", Applied Optics 33, 5451-5466 (1994).
(3) C.P. Williams and S.H. Clearwater, *Explorations in Quantum Computing*, Springer-Verlag, New York, 1997.

(4) C.P. Williams and S.H. Clearwater, *Ultimate Zero and One*, Springer-Verlag, New York, 2000.
(5) J.D. Howell and J.A. Yeazell, "Quantum Computation through Entangling Single Photons in Multipath Interferometers", Phys. Rev. Letters 85, 198-201 (2000).
(6) S. Takeuchi, "Experimental Demonstration of a Three-Qubit Quantum Computation Algorithm using a Single Photon and Linear Optics", Phys. Rev. A 62, ___ (2000).
(7) C.H. Bennett and G. Brassard, *in Proc. IEEE Int. Conference on Computers, Systems and Signal Processing*, IEEE Press, New York (1984); G. Gilbert, and M. Hamrick, "Practical Quantum Cryptography: A Comprehensive Analysis (Part One)", Mitre Technical Report MTR00W0000052, September 2000.
(8) G.S. Vernam, "Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications, " J. Amer. Inst. Elect. Eng. **XLV**, 109-115 (1926).
(9) C. Maurand and P. D. Townsend, "Quantum key Distribution Over Distances as Long as 30 km", Optics Letters 20, 1695-1697 (1995); P.D. Townsend, "Simultaneous Quantum Cryptographic Key Distribution and Conventional Data Transmission Over Installed Fibre using Wavelength-Division Multiplexing", Electronics Letters 33, 188-190 (1997).
(10) Marco Listanti and Roberto Sabella, "Optical Networking Solutions for Next-Generation Internet Networks, IEEE Communications Interactive, September 2000; Daniel Blumenthal, "Routing Packets with Light," Scientific American, 96-99, January 2001.